



(12) 发明专利申请

(10) 申请公布号 CN 115989495 A

(43) 申请公布日 2023.04.18

(21) 申请号 202180048896.9

(22) 申请日 2021.07.08

(30) 优先权数据

20185298.5 2020.07.10 EP

(85) PCT国际申请进入国家阶段日

2023.01.09

(86) PCT国际申请的申请数据

PCT/EP2021/069077 2021.07.08

(87) PCT国际申请的公布数据

W02022/008692 EN 2022.01.13

(71) 申请人 纳格拉影像有限公司

地址 瑞士舍索-苏尔-洛桑

(72) 发明人 S·佩利西耶 P·奥布里

(74) 专利代理机构 中国贸促会专利商标事务所
有限公司 11038

专利代理师 张丹

(51) Int.Cl.

G06F 21/75 (2006.01)

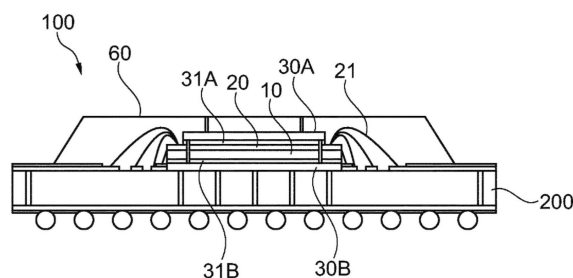
权利要求书1页 说明书7页 附图3页

(54) 发明名称

针对恶意攻击具有保护功能的集成电路器件

(57) 摘要

本发明提供了针对恶意攻击具有保护功能的集成电路器件。集成电路器件(100)包括半导体基板层(10)和至少一个有源层(20),该至少一个有源层包括电子部件并且由所述半导体基板层(10)支撑。半导体基板层(10)和至少一个有源层(20)被夹置在两个保护层(30A,30B)之间,该两个保护层用作物理障碍物以防止辐射的通过。另外,两个保护层(30A,30B)电连接至检测电路(40),该检测电路能够监测保护层(30A,30B)的电信息并且基于所监测的电信息来检测两个保护层(30A,30B)中的至少一个保护层的物理攻击。



1. 一种集成电路器件(100),所述集成电路器件包括半导体基板层(10)和至少一个有源层(20),所述有源层包括电子部件并且由所述半导体基板层(10)支撑,其特征在于,所述半导体基板层(10)和所述至少一个有源层(20)被夹置在两个保护层(30A,30B)之间,所述两个保护层用作物理障碍物以防止辐射的通过并且电连接到检测电路(40),所述检测电路用于监测所述保护层(30A,30B)的电信息并且基于所监测的电信息来检测所述两个保护层(30A,30B)中的至少一个保护层的物理攻击。

2. 根据权利要求1所述的器件,其特征在于,所述检测电路(40)被集成在所述至少一个有源层(20)内。

3. 根据权利要求1或2所述的器件,还包括电子保护电路(50),所述电子保护电路被配置为当所述检测电路(40)检测到物理攻击时生成用于执行电子保护对策的信号。

4. 根据权利要求3所述的器件,其特征在于,所述电子保护电路(50)被集成在所述至少一个有源层(20)内。

5. 根据权利要求1至4中任一项所述的器件,其特征在于,所述两个保护层(30A,30B)被配置为防止包括激光辐射、来自所述至少一个有源层的电磁放射、由外部源产生的电磁辐射的组中的辐射的通过。

6. 根据权利要求1至5中任一项所述的器件,其特征在于,所述两个保护层由金属、或金属合金或半导体材料制成。

7. 根据权利要求1至6中任一项所述的器件,其特征在于,所述保护层(30A,30B)中的至少一个保护层是全板。

8. 根据权利要求1至7中任一项所述的器件,其特征在于,所述保护层(30A,30B)中的所述至少一个保护层由形成平行线的弯曲连续导线制成。

9. 根据权利要求1至8中任一项所述的器件,其特征在于,所述两个保护层(30A,30B)中的每个保护层都包括电连接到所述检测电路(40)的基本板的拼接。

10. 根据权利要求1至9中任一项所述的器件,其特征在于,所述检测电路(40)被配置为测量所述两个保护层(30A,30B)的相应电气值之间的相对值。

11. 根据权利要求1至10中任一项所述的器件,其特征在于,所述检测电路(40)被配置为测量所述两个保护层(30A,30B)之间的电容,所述电容作为所述两个保护层(30A,30B)的所述电信息。

12. 根据权利要求1至10中任一项所述的器件,其特征在于,所述检测电路(40)被配置为测量所述两个保护层(30A,30B)之间的电阻差,所述电阻差作为所述两个保护层(30A,30B)的所述电信息。

13. 根据权利要求1至12中任一项所述的器件,其特征在于,所述检测电路(40)被配置为检测所监测的电信息相对于参考值在公差范围之外的偏差。

14. 根据权利要求1至13中任一项所述的器件,其特征在于,所述两个保护层(30A,30B)通过用作电绝缘体的两个相应的接合层(31A,31B)接合到所述半导体基板层(10)和所述至少一个有源层(20)。

15. 一种产品,所述产品包括根据权利要求1至14中任一项所述的集成电路器件。

针对恶意攻击具有保护功能的集成电路器件

技术领域

[0001] 本公开涉及针对恶意攻击(如侧信道攻击和故障攻击)的集成电路保护领域。

背景技术

[0002] 在计算机安全中,通常由被设计成在数学上极难破解的密码算法来提供安全性。攻击者可获得输入和输出消息,但无法获得秘密信息(例如,加密算法的秘密密钥)。对于经过充分研究的算法,攻击者必须执行密码分析,其需要不切实际的计算能力才来获得秘密信息。

[0003] 然而,已经表明,密码算法或协议的硬件和软件实现易受到不需要如此复杂的密码分析的侧信道攻击和故障攻击的影响。这两种技术都可用于获得存储在诸如实现密码算法的集成电路的嵌入式设备中的秘密信息(例如,秘密密钥)。

[0004] 侧信道攻击是基于秘密信息可以通过侧信道泄漏的原理。其能够被定义为基于从计算机系统的实现获得的信息的任何攻击,而不是所实现的算法本身的弱点。侧信道是物理信息泄漏,例如执行加密所需的时间、执行加密算法所消耗的硬件实现的功率、从执行加密或解密的电路发出的电磁辐射,或甚至是声音。事实证明侧信道攻击十分有效,并且需要低成本和/或减少的实验次数。

[0005] 故障攻击在于故意地触发密码算法中的计算故障以获得故障输出或故障行为,从而获得秘密信息。使用例如激光源或电磁源的故障注入用于改变密码器件的行为并且在故障环境下获得信息泄露。例如,体偏置注入(Body Bias Injection,BBI)是一种故障注入方法,其在于在电路基板上施加高压脉冲以诱发故障。

[0006] WO 96/16378A1公开了一种安全器件,该安全器件包括第一集成电路和第二集成电路,第一集成电路具有存储秘密信息的存储器区域,第二集成电路布置在第一集成电路上方并且覆盖存储器区域(以及任何其他敏感电路)以形成障碍并防止对存储器区域的访问。两个集成电路通过粘合剂层接合在一起并且被连接以便彼此通信。在操作中,在两个集成电路之间建立周期性通信以执行相互认证过程。如果两个集成电路中的一个集成电路未能通过认证,则从存储器区域擦除秘密信息。为了访问存储器区域,攻击者需要移除第二集成电路,这会导致两个集成电路之间的连接中断。

[0007] US 5,881,155 A公开了一种用于防止访问存储在包括第二半导体芯片(保护芯片)的半导体芯片(受保护芯片)中的秘密信息的安全器件。两个芯片通过通信端子彼此耦合。具有非均匀电阻率的半导体树脂被夹置在受保护芯片与保护芯片之间。保护芯片具有测量通过树脂的多个电阻的装置和通过处理所测量的电阻来确定加密密钥(“电阻密钥”)的装置。当安全器件被初始化时,测量装置通过半导体树脂来测量一定数值的电阻。然后对电阻的测量值进行处理,以确定通过通信终端被传送到受保护船舶的电阻密钥,以便加密和解密信息。在该配置中,对受保护芯片的物理攻击将不提供对秘密信息(电阻密钥)的访问。此外,其先决条件是接近芯片的有源表面并因此破坏半导体层,这永久地阻止了电阻密钥的重构。

[0008] WO 99/12204A1公开了一种安全集成电路,该安全集成电路包括通过中间密封层连接在一起的有源层和互补层。“有源”层包括半导体材料的基板子层,以及在基板子层上方的集成电子电路并具有存储器的有源子层。该有源层被减薄。互补层由半导体材料制成。中间密封层由电绝缘材料制成。当攻击者想要访问集成电路时,该攻击者需要通过施加牵引力将互补层与有源层分离。当有源层变薄并因此弱化时,这样的牵引力将不可避免地破坏有源层,这将使得提取秘密信息变为不可能。

[0009] 现有技术的安全器件在实现和设计上十分复杂。此外,其仅针对来自芯片一侧的物理攻击提供保护。然而,最近已经表明,来自芯片两侧的攻击是可行的。此外,现有技术的安全器件被设计成防止从存储器读取秘密信息,但不提供针对侧信道攻击、电磁故障攻击或体偏置注入攻击的有效保护。

[0010] 有必要改善该情况。

发明内容

[0011] 本公开涉及一种集成电路器件,该集成电路器件包括半导体基板层和至少一个有源层,该有源层包括电子部件并且由所述半导体基板层支撑,其特征在于,半导体基板层和至少一个有源层被夹置在两个保护层之间,该两个保护层用作物理障碍物以防止辐射的通过并且电连接到检测电路,该检测电路用于监测保护层的电信息并且基于所监测的电信息来检测两个保护层中的至少一个保护层的物理攻击,以便保护至少一个有源层免受物理攻击。

[0012] 根据本公开,集成电路器件在芯片(集成电路)的两侧上使用保护层或屏蔽层。该两个保护层作为物理障碍,防止内部和/或外部辐射的通过。这种配置产生的保护可与“法拉第笼”效应相比较。该保护防止使用来自芯片两侧的辐射(例如,激光束或电磁干扰)的侵入性攻击。其还基于对从有源层发出的电磁辐射的检测来防止侧信道攻击。

[0013] 另外,在攻击者试图去除保护层中的一个保护层的全部或部分的情况下,检测电路基于所监测的保护层的电信息来检测攻击,并触发电子保护对策,例如存储器擦试。

[0014] 因此,在本公开中,保护层用作物理屏蔽以保护集成电路免受使用辐射的攻击,并且还用作触发器以在集成电路器件通过挖掘保护层而受到物理攻击的情况下激活电子保护对策。因此,本公开结合了物理保护和电子保护对策,两者都允许保护有源层免受恶意攻击。物理保护在实际中被用作执行电子对策的触发器。

[0015] 有利地,检测电路被集成在至少一个有源层内。

[0016] 集成电路器件还可以包括电子保护电路,该电子保护电路被配置为当检测电路检测到物理攻击时生成用于执行电子保护对策的信号。

[0017] 有利地,电子保护电路被集成在至少一个有源层内。

[0018] 两个保护层能够被配置为防止包括激光辐射、来自至少一个有源层的电磁放射、由外部源(即,在集成电路器件外部)产生的电磁辐射的组中的内部和外部辐射的通过。

[0019] 两个保护层能够由金属、或金属合金或半导体材料制成。

[0020] 在第一实施方案中,集成电路器件被设计用于引线接合。

[0021] 在第二实施方案中,集成电路器件是倒装芯片系统。

[0022] 两个保护层中的一个保护层或两个保护层中的每个保护层可为全板。

[0023] 在第一变型中,两个保护层中的个保护层或两个保护层中的每个保护层由形成平行线的弯曲连续导线制成。可选地,该弯曲连续导线可由印刷电路板支撑。

[0024] 在另一个实施方案中,保护层包括电连接到检测电路的基本板的拼接。

[0025] 检测电路可被配置为测量两个保护层的相应电气值之间的相对值。

[0026] 在第一示例中,检测电路被配置为测量两个保护层之间的电容,作为两个保护层的所述电信息。

[0027] 在第二示例中,检测电路被配置为测量两个保护层之间的电阻差,作为两个保护层的所述电信息。

[0028] 检测电路被配置为检测所监测的电信息相对于参考值在公差范围之外的偏差。

[0029] 可选地,两个保护层通过用作电绝缘体的两个相应的接合层接合到半导体基板层和至少一个有源层。

[0030] 本公开还涉及包括集成电路器件的产品。

附图说明

[0031] 通过阅读参考附图所作的非限制性实施方案的详细说明,本公开的其他特征、目的和优点将变得更加清楚。

[0032] 图1示出了根据第一实施方案的集成电路器件。

[0033] 图2示出了根据第二实施方案的集成电路器件。

[0034] 图3示出了向集成电路器件提供电子保护的电子电路。

[0035] 图4A、图4B示出了根据第一实施方案的集成电路器件的第一变型。

[0036] 图5示出了根据第一实施方案的集成电路器件的第二变型。

[0037] 图6示出了集成电路器件的第三实施方案。

[0038] 图7是示出根据第一实施方案的集成电路器件的操作的组织图。

具体实施方式

[0039] 本公开涉及一种集成电路器件,该集成电路器件被设计为提供针对恶意攻击的保护,特别是针对侧信道攻击和故障攻击的保护。

[0040] 集成电路器件是可经设计以执行密码算法和/或协议的硬件与软件实现的混合。这些硬件和软件实现易受侧信道攻击和故障攻击(例如,利用激光束的故障攻击或短时脉冲干扰电磁攻击)的影响。这种攻击可以基于使用辐射来将故障注入到集成电路器件中并改变其行为,或者基于对从电路发出的辐射的检测。本公开旨在提供针对使用指向电路的外部辐射源(例如,激光或电磁干扰)的攻击以及基于从电路发出的辐射检测到的攻击的保护。

[0041] 如本领域技术人员所公知的,集成电路器件100包括多个重叠层,该多个重叠层包括半导体基板层10和至少一个有源层20。半导体基板层10由半导体材料制成。有源层20包括电子部件,诸如半导体部件。该有源层还包括导电迹线。可以在这些有源层中集成一个或多个电子电路或器件。

[0042] 在本公开中,半导体基板层10和有源层20被夹置在用作物理障碍物的两个保护层或“屏蔽”层30A、30B之间,以防止内部和外部辐射的通过。保护层设置在层10、20的叠层的

两侧(图1或图2中的顶部和底部)上。其构成附加的重叠层。这些保护层被设计成防止诸如激光辐射和电磁辐射的辐射的通过。其产生可与用于保护集成电路器件100(特别是有源层)的“法拉第笼”效应相比较的效应。例如,由外部源(即,在集成电路器件外部)发射并且被引导朝向集成电路器件的激光束撞击保护层中的一个保护层并且被该保护层阻挡。在集成电路器件的一侧上出现电磁故障的情况下,电磁场撞击布置在该侧上的保护层并且像法拉第笼那样分布在该保护层上,而不破坏有源层。此外,保护层吸收来自电路的辐射,诸如来自电路的电磁放射。其结果是,通过侧信道攻击来获得秘密信息非常困难,甚至是不可能的。

[0043] 每个保护层30A、30B的厚度可适于提供有效的保护。厚度值可取决于一个或多个参数,诸如保护层的材料和集成电路器件所需的尺寸,并且可通过实验来确定。例如,对于给定的保护层材料,该厚度可在50 μm 和200 μm 之间,以便提供良好的保护和缩小的尺寸。然而,对于另一种材料,较薄的厚度(例如,30 μm)也可能同样有效。如果对集成电路器件的尺寸没有要求,也可以采用高于200 μm 的厚度。例如,每个保护层的厚度可以等于500 μm 。

[0044] 保护层30A、30B可由金属制成,例如铜或铝或金或铂。或者,该保护层由金属合金,诸如不锈钢(例如,300级不锈钢)或半导体材料制成。

[0045] 保护层30A、30B提供针对侧信道攻击、激光攻击和电磁攻击(诸如电磁故障攻击和体偏置注入攻击)的强被动保护。实际上,这些屏蔽层30A、30B在集成电路器件100的两侧上保留大部分(如果不是全部)电磁放射,使得获取侧信道数据非常困难。其还保持朝向有源层的任何激光束,并且大部分电磁信号或针朝向有源层,使其很难以干扰集成电路的操作。

[0046] 接合层或界面层31A、31B能够分别插置在保护层30A、30B与层10和20之间,以便促进保护层的粘附。这些接合层31A、31B具有将保护层30A与有源层20接合、将保护层30B与半导体基板层10接合的功能。其可由本领域技术人员公知的特定胶制成。接合层的材料可为如本领域技术人员所公知的电绝缘材料。保护层30A、30B可以以另一种方式接合到层10和20。

[0047] 如图3中示意性示出的,保护层30A、30B电连接到检测电路40。该检测电路或器件40具有监测保护层30A、30B的电信息并且基于所监测的电信息来检测两个保护层30A、30B中的至少一个保护层的物理攻击的功能。检测电路40被集成在集成电路器件100的有源层20中。每个保护层30A、30B通过一个或多个TSV(硅通孔)连接到检测电路40。

[0048] 更准确地说,检测电路40能够被配置为监测两个保护层30A、30B之间的相对电气值。这样的相对值预计会随着时间保持恒定或几乎恒定。特别地,集成电路器件100的温度变化不应该对该相对值产生影响。

[0049] 相对电气值可为两个保护层30A、30B之间的电容。另外,相对电气值可为两个保护层之间的电阻差。

[0050] 检测电路40被配置为测量两个保护层30A、30B之间的相对电气值,并且通过确定该相对电气值随时间是否保持恒定或几乎恒定来监测该相对电气值,以便检测物理攻击。为此,检测电路40可使用包括参考值的公差范围。所监测到的相对电气值在该公差范围内的变化可被接受,而所监测到的相对电气值在公差范围外的变化可被检测电路40检测为物理攻击。换句话说,如果所测量的相对电气值在该公差范围内,则认为其保持恒定(或几乎恒定)并且没有检测到物理攻击。但是,如果所测量的相对电气值在公差范围之外,则认为

其不保持恒定并且检测到物理攻击。可以通过实验来表征公差范围,以便允许对攻击有效检测并且避免错误检测。例如(仅),可以容忍与参考值相比增加或减少10%的变化(被认为是“几乎恒定的”)。然而,该 $\pm 10\%$ 的值仅为示例。其他公差范围可酌情确定,例如与参考值相比 $\pm 5\%$ 或 $\pm 30\%$,或者任何其他的通过实验确定的适于有效检测攻击和避免错误检测的值。

[0051] 如图3所示,集成电路器件100还包括电子保护电路50。该保护电路50与检测电路40连接。在操作中,当集成电路器件受到物理攻击时,通过挖掘保护层30中的一个保护层,该物理攻击被检测电路40检测到,并且向保护电路50发出信号。由此,保护电路50生成用于执行电子保护对策的控制信号。例如,控制信号是擦除一个或多个存储器、或阻挡集成电路器件的操作(功能)的命令、或旨在保护集成电路器件100的秘密或敏感信息的任意其他对策。

[0052] 由于检测电路40和保护电路50,保护层30A、30B不仅用作无源保护以阻挡进入集成电路(芯片)的激光或电磁信号或芯片外的电磁放射,而且当集成电路器件100受到物理攻击并且攻击者试图去除保护层30A、30B中的一个保护层的全部或部分时,用作触发主动对策的部件。

[0053] 集成电路器件100还可包括覆盖该组重叠层10、20、30A、30B、31A、31B的模制罩60。

[0054] 集成电路器件100可由载体200支撑。该载体200可支撑集成电路器件100的电路所连接到的导电迹线。这种配置允许导电迹线的重新分布,以便集成电路器件100与其他电子器件连接。该载体200可由支撑其他电子部件或器件的另一较大载体(未示出)支撑。如图1和图2所示,载体200与较大载体之间的电连接可使用焊球端子。

[0055] 第一实施方案

[0056] 图1示出了被设计用于引线接合的集成电路器件100的第一实施方案。集成电路器件100是引线接合封装件。该实施方案符合上述公开内容。现在将参照图1描述该第一实施方案特有的特征。

[0057] 如本领域技术人员所公知的,由于集成电路器件100的第一实施方案被设计用于引线接合,例如由Au制成的多根连接线21,将有源层20的电路连接到由载体200支撑的导电迹线,以用于连接的重新分布。集成电路器件100的层从载体200到模制罩60(即,在图1中从底部到顶部)按照以下顺序彼此重叠:保护层30B、接合层31B、半导体基板层10、有源层20、接合层31A和保护层30A。

[0058] 根据第一实施方案,保护层30A、30B是两个板,有利地是两个全板。

[0059] 现在将参照图7描述集成电路器件100(例如,图1中所示的集成电路器件)的操作。

[0060] 两个保护层30A、30B用作物理障碍物以防止辐射的通过。其防止诸如激光束或电磁辐射的辐射通过。在攻击者通过将激光束从外部激光源导向有源层而攻击集成电路器件100的情况下,该激光束被保护层30A、30B中的一个保护层止挡。在从集成电路器件100的一侧进行短时脉冲干扰电磁攻击的情况下,设置在该侧上的保护层30附近产生的电磁场被该保护层阻挡,并且不会干扰有源层20。此外,在侧信道攻击的情况下,保护层30A、30B止挡在操作中由电路产生的电磁放射,使得攻击者无法捕获这些电磁放射以获得秘密信息。

[0061] 在步骤S1中,检测电路40测量两个保护层30A、30B之间的相对电气值。当集成电路器件100被供电时,可在集成电路器件100的寿命期间进行这种监测。例如,两个保护层30A、

30B被认为是两个电容器,并且测量两个保护层30A、30B的相应电容值之间的差C。由于所测量的电气值是两个保护层之间的“相对”值,因此预期其随时间恒定(或几乎恒定)。即使温度升高,两个电容器也将类似地受到影响,不应当由温度的变化进行修改。然而,在相对于参考值的公差范围内(例如,相对于参考值增加或减少10%)可以容忍较小的变化。在监测步骤S2中,监测两个保护层30A、30B之间的所测量的相对电气值(例如,电容C的差),以便确定其是否偏离参考值“Co”在公差范围之外。检测电路40确定所测量的相对电气值C与参考值Co相比是否保持恒定或在预定的公差范围内。如果是(图7中的分支Y),则检测器件40重复步骤S1和S2。没有检测到物理攻击。

[0062] 在集成电路器件100的物理攻击的情况下,攻击者应该在访问有源层之前挖掘两个保护层中的至少一个保护层。在这种情况下,检测电路40在步骤S2(图7中的分支N)中检测到所测量的相对电气值C改变并且偏离参考值超出公差范围。其结果是,在步骤S3中,检测电路40生成警报信号,并且在步骤S4中将该警报信号发送到电子保护电路50。例如(仅),当所监测的相对电气值与参考值相比增加或减少超过10%时,由检测电路40生成警报信号。

[0063] 在接收到警报信号时,电子保护电路50在步骤S5中控制电子对策的执行以保护集成电路器件100。对策可以是以下动作中的一者或多者:擦除集成电路器件100的一个或多个存储器、阻挡集成电路器件100的操作、或者本领域技术人员已知的任何其他电子对策。

[0064] 代替电容,可以测量和监测两个保护层30A、30B的相应电阻值之间的差。可替换地,即使在温度变化的情况下,预期保持恒定或几乎恒定的两个保护层30A、30B的任何其他电特性也可以由检测电路40来测量和监测。

[0065] 如前所述,保护层30A、30B提供针对诸如侧信道攻击和故障攻击等攻击的物理保护和被动保护。其结果是,攻击者需要去除两个保护层30A、30B中的至少一个保护层的全部或部分。在保护层30中的一个保护层中钻孔,或整体地移除保护层30中的一个保护层,将具有触发执行如存储器擦试的对策的安全机制的效果。安全机制可以是任何类型,并且本公开不限于某些特定的对策。

[0066] 第一实施方案的变型1

[0067] 在第一实施方案的变型中,两个保护层30A、30B中的至少一个保护层(即,其中的任一者或两者)能够由弯曲以形成平行线的单根连续导线32制成。

[0068] 图4A和图4B示出了第一实施方案的该第一变型的示例。在该示例中,集成电路器件100的结构类似于第一实施方案的结构,但使用一根弯曲连续导线32A、32B来替代每个保护板并且起到保护或屏蔽层30A、30B的作用。如先前在第一实施方案中所述,弯曲连续导线32、32B能够通过接合(界面)层31A、31B接合到有源层或半导体基板层。因此,每根弯曲导线32A、32B在相应的接合层31A、31B上方延伸。

[0069] 图4A是集成电路器件100的重叠层30A、31A、20、10、31B、30B的俯视图。其示出了由单根弯曲导线32A形成的保护层30A。图4B示出了重叠层30A、31A、20、10、31B、30B的侧视图。

[0070] 在每个保护层30A、30B中,导线的平行线彼此之间非常接近。两条相邻线之间的空间可以非常小,例如几微米。

[0071] 类似于全板,每根弯曲导线32A(32B)形成保护集成电路器件免受攻击的屏蔽。另外,屏蔽件由单根导线提供,这一事实有利于在屏蔽件受到攻击时进行检测。实际上,检测

导线是否已被切断非常容易。

[0072] 第一实施方案的变型2

[0073] 第一实施方案的第二变型类似于上述第一实施方案,而不同之处仅在于每根弯曲连续导线32A (32B) 是由印刷电路板 (PCB) 33 (指集成电路器件的一侧33A和另一侧33B) 支撑的。印刷电路板33A (33B) 在保护层30A (30B) 与接合层31A (31B) 之间形成中间层。导线32A (32B) 印刷在相应的PCB 33A (33B) 上。这可以改善物理保护。由这种配置所提供的针对不同攻击的保护非常接近于由全板所提供的保护。

[0074] 承载弯曲连续导线的印刷电路板可设置在集成电路器件的一侧或两侧上。

[0075] 保护层的第一变型和第二变型可以用在根据第一实施方案的集成电路器件中,也可以用在设置有助于互连到适于接收这种保护层的外部电路的另一接口的集成电路器件中。

[0076] 第二实施方案

[0077] 如图2所示,集成电路器件的第二实施方案与第一实施方案的不同之处在于其是倒装芯片系统。

[0078] 焊球端子70将有源层20的电路连接到由载体200支撑的导电迹线,用于重新分布有源层的连接端子。按照以下顺序从载体200到模制罩60 (在图2中从底部到顶部) 布置重叠层:保护层30A、接合层30A、有源层20、半导体基板层10、接合层31B和保护层31B。如本领域技术人员所公知的,未在图2中示出的圆柱形导电柱 (例如,由铜制成) 插置在焊球端子70与有源层20的连接端子之间,并且布置为穿过设置在保护层30A中的孔。

[0079] 根据第二实施方案的集成电路器件的操作类似于根据第一实施方案的集成电路器件的操作。

[0080] 第三实施方案

[0081] 在第三实施方案中,每个保护层30都包括基本板的拼接,如图6所示的基本板34A。每个基本板34A (例如,通过TSV) 电连接到检测电路40。两个保护层30A和30B完全相同。这意味着第一保护层30A的每个基本板34A面对第二保护层30B的相应的基本板34B。彼此面对的两个相应的基本板34A、34B耦合。

[0082] 在操作中,检测电路40测量每对基本板34A、34B的两个耦合的基本板之间的相对电气值。例如,检测电路40被配置为测量两个耦合的基本板之间的电容或者两个耦合的基本板的相应电阻之间的差。

[0083] 保护层的这种配置可以用在引线接合封装件 (第一实施方案) 中的集成电路器件中,或者用在倒装芯片系统 (第二实施方案) 中,或者用在设置有助于互连到外部电路的另一类型接口的集成电路器件的另一封装件中。

[0084] 在变型中,如前所述,基本板34A (34B) 可以由印刷电路板支撑。

[0085] 集成电路器件100能够集成于产品中。本公开还涉及这样的产品。

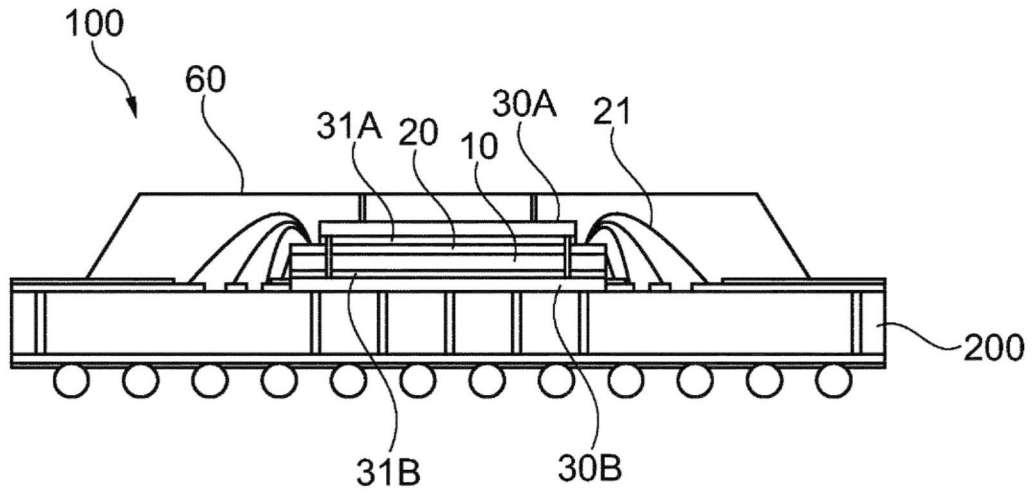


图1

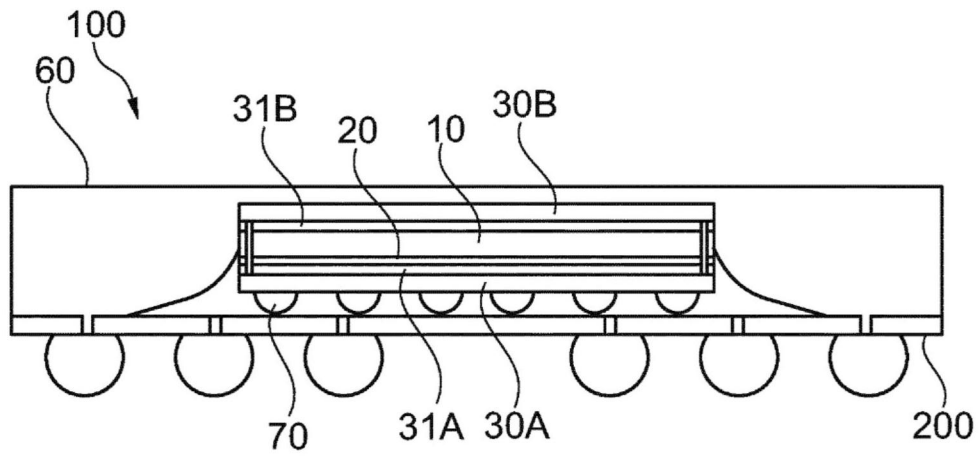


图2

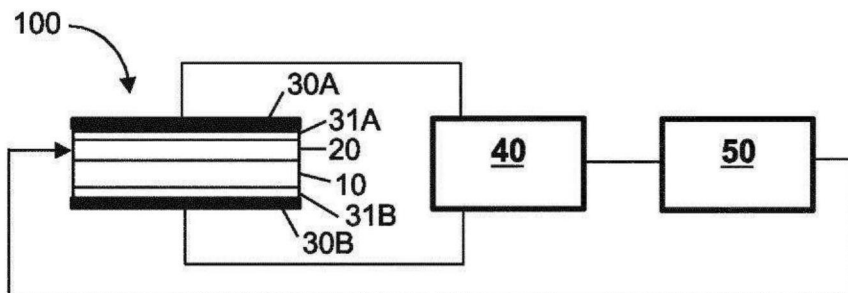


图3

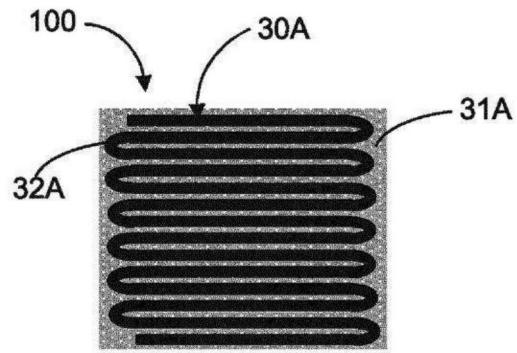


图4A

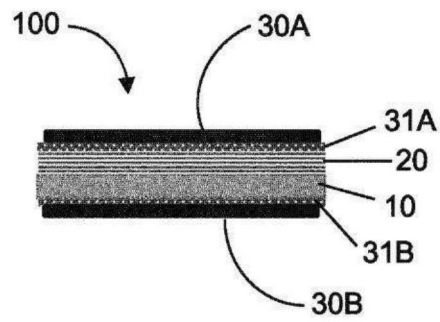


图4B

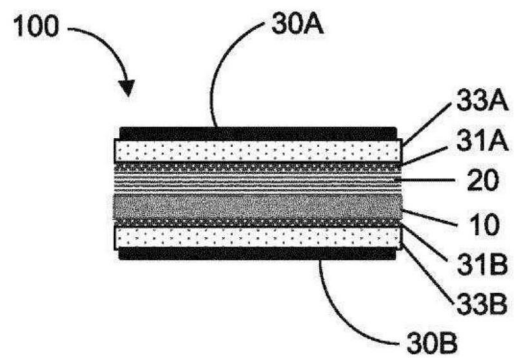


图5

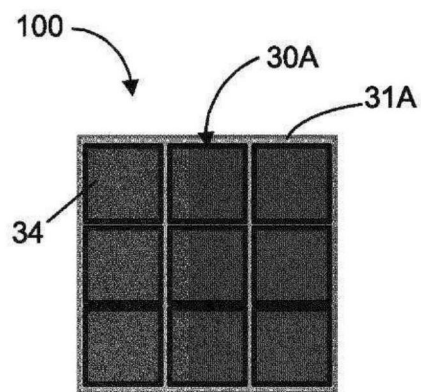


图6

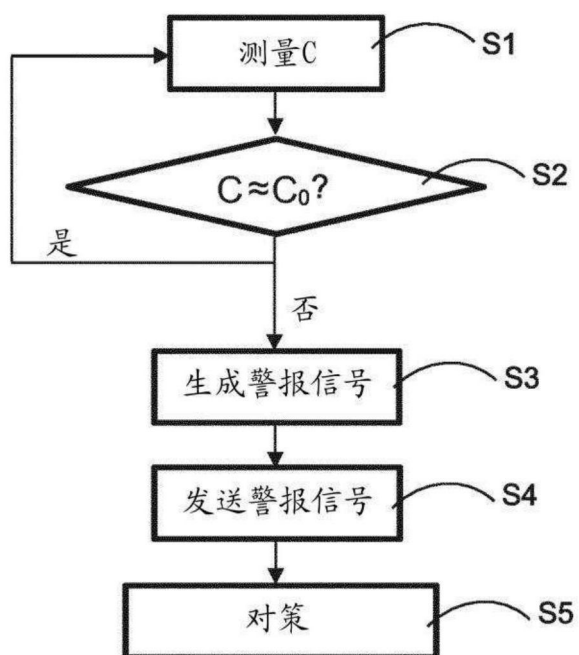


图7